IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 7, 2020, accepted January 27, 2020, date of publication February 4, 2020, date of current version February 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2971604

A Systematic Literature Review of Fraud Detection Metrics in Business Processes

BADR OMAIR AND AHMAD ALTURKI

Department of Information Systems, Faculty of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding author: Badr Omair (balomair@gmail.com)

This work was supported by the Deanship of Scientific Research (DSR), King Saud University, Riyadh, Saudi Arabia, through the Initiative of DSR Graduate Students Research (GSR).

ABSTRACT Fraud is a primary source of organization losses, amounting to up to 5% of yearly revenues. Process-based fraud (PBF) is fraud involving a deviation from the standard operating procedure (SOP) of business processes. PBF hinders the achievement of business objectives because business processes operationalize organizational strategies. A systematic content analysis of the literature was conducted on fraud detection metrics in business processes. The current state of fraud detection was surveyed by focusing on PBF metrics while including all relevant conceptual perspectives of PBF detection. The findings indicate that a large body of research has examined detection metrics for possible fraud, but less attention has been paid to PBF. In addition, the currently available PBF detection metrics do not adequately address the needs of different conceptual perspectives on business processes. For example, metrics may be undefined for one or more of the following: components of a business process, business process perspectives, critical information for auditing the business process, and business process presentation layers. This paper addresses these gaps by paying attention to PBF and various conceptual perspectives for a successful PBF detection approach.

INDEX TERMS Business process fraud, fraud detection, fraud indicators, fraud metrics, process-based fraud, systematic literature review.

I. INTRODUCTION

Awareness of fraud and its corresponding countermeasures has increased after several instances of fraud were exposed in the early part of the 21st century (e.g., Enron in 2001, MCI WorldCom in 2002, Parmalat in 2003, Lehman Brothers in 2008, Fannie Mae in 2008, Satyam in 2009, Olympus in 2011, and HRE in 2011) [1], [2]. The collapse of Enron created a loss of approximately $70 billion in the capital markets [3]. In 2017, the Annual Fraud Indicator showed that fraud-related losses to the UK economy were estimated at £190 billion [4].

Financial devastation and a tarnished reputation are the most obvious effects of fraud on organizations [5]. Fraud ultimately leads to increased costs while damaging customer experience and external relations [5]. Fraudulent incidents have escalated in recent years [6], thus creating a severe problem globally [7].

Fraud is difficult to prevent and detect [8] because it is an irregular, imperceptibly hidden, time-evolving, and usually carefully planned crime that can take many forms [9]. Nonetheless, implementing fraud detection techniques can help organizations identify and recognize fraud [8]. Detecting fraud has become a priority in organizations [10] because anti-fraud systems are ill-equipped to prevent every case of fraud [11].

The Association of Certified Fraud Examiners[1] (ACFE) defines occupational fraud as an employee's use of his or her job for personal enrichment through the intentional abuse or misapplication of the employing organization's resources or assets [12]. Occupational fraud includes fraud in business processes, known as process-based fraud (PBF) [13].

The associate editor coordinating the review of this manuscript and approving it for publication was Mervat Adib Bamiah.

[1] https://www.acfe.com.

Business processes are a set of activities combined to achieve business goals [14]. They involve systems, data, and resources that may exist inside or outside an organization [15]. Also, business processes performed within a single organization may involve cooperation with other organizations [14]. These processes are critical because they are the backbone of the organization's business [16] and determine revenue. In addition, business processes shape the cost profile of an organization [15] because, directly or indirectly, they usually affect the financial accounts [17].

Because business processes are crucial to businesses, PBF awareness and detection should be a top management concern [18]. However, the scale of fraudulent manipulations is vast and continues to increase [19]. Moreover, PBF detection is not well addressed [11].

This study involved a systematic literature review of fraud detection metrics[2] in business processes. Content analysis was used to survey the existing PBF detection metrics and examine whether they address all the conceptual perspectives on business processes. The study is organized as follows: Section 2 provides a background to the literature review study, Section 3 explains the literature review method and results, and Section 4 offers conclusions.

II. BACKGROUND

In general, measurement is defined as the process of assigning numbers or symbols to attributes (such as possible fraud metrics) of entities (such as business processes) using well-defined rules [20]. Metrics are observable values that emerge from a measurement. Business process measurement is "the task of empirically and objectively assigning numbers to the properties of business processes. . . to describe them" [21]. Thus, detection metrics for possible PBF are the observable values from the appropriate measurements of the business process. These metrics should include all fraud-related properties of business processes.

Business process measurement involves the following tasks [22]–[24] as cited in [25]:

- Selecting a measurement framework that describes how the measurement should be carried out in general.
- Defining the metrics used in the measurement process.
- Specifying the data sources for the measurement.
- Considering the implications of the business process context, such as weather conditions and holiday seasons.

Metrics can be defined by applying the following steps [26]:

- Identifying the measured entity, namely, the business process in this study.
- Identifying the attributes of the entity to be measured (such as process-performance anomaly attributes that can be used for detecting fraud).
- Defining the metric (such as anomalous process execution time, which may indicate possible fraud in the business process).

The most important criteria for defining useful process metrics are as follows [27]:

- ***Accuracy:*** a metric should reflect reality by precisely specifying the relationship between the metric and its underlying attributes.
- ***Cost-effectiveness:*** the cost of using a metric should reflect the value derived from it.
- ***Easy to understand:*** a metric's stakeholders should need to make only a basic cognitive effort to comprehend its use.
- ***Timeliness:*** a metric should be available fast enough (within a reasonable timeframe) to take action based on the analytical information it provides.
- ***Actionable:*** there should be a clear relationship between the actions of decision-makers and the observed metric; for example, a metric should help decision-makers identify the cause of the problem.

A metric can be atomic (independent) or composite when the metric itself depends on other metrics [28]. Moreover, the metric value alone may not be enough for evaluating the measured property. The value may require comparison with other values or a threshold (limit) to be useful [28].

Metrics can be validated theoretically and empirically [29]. Theoretical validation might involve, for example, examining the properties of the measurement scale (that is, nominal, ordinal, interval, ratio, and absolute). Empirical validation could involve conducting a survey, experiment, or a case study. Both validations are essential to determine whether a metric is valid, precise, useful, and that it measures what it is intended to measure [29]. Most researchers agree that theoretical and empirical validations are necessary for defining metrics [29]. Additionally, the development of an IT tool for automatic metric calculations is considered an optional part of defining a metric [28].

The study of detection metrics for possible PBF is part of two main disciplines: fraud risk management and business process management (BPM). They are described below:

A. FRAUD RISK MANAGEMENT

Fraud risk management is the process of managing all fraud risks in the organization. This includes evaluating potential fraud risks associated with business processes to ensure the achievement of business objectives [18]. Fraud risk management embraces both fraud detection and fraud prevention, which are necessary for an effective strategy to combat fraud [8]. Whereas fraud detection aims to discover and recognize any fraudulent activities, fraud prevention seeks to avoid or reduce fraud. Both are independent and should be aligned and considered jointly [8].

The fraud triangle theory [30] offers a universal model for describing and understanding key fraud characteristics [31].

[2] The terms "indicator," "measure," and "metric" are typically used interchangeably [76]. However, "metric" is used in this study because it is a general term clearly expressing the value of the measurement process.

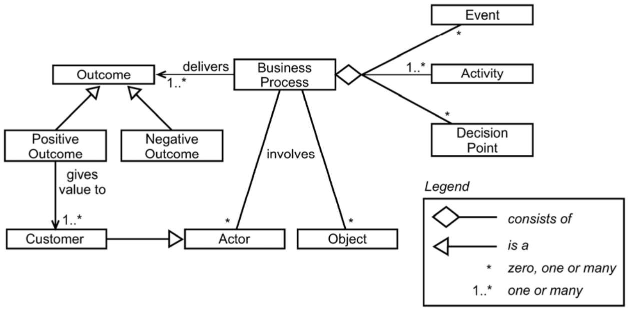

FIGURE 1. **Ingredients of the business process. Source: [15].**

The fraud triangle theory states that fraud is more likely when three factors are present: pressure or incentives, opportunity, and attitude or rationalization. The factors are described as follows [3]: First, to conduct fraud, the perpetrator must have an incentive or pressure to commit fraud (an employee might have a financial or another type of obligation). Second, the perpetrator can commit fraud by taking advantage of weak internal control systems, inadequate security of company assets or unclear policies concerning acceptable behavior. Finally, the perpetrator rationalizes the fraudulent behavior (an employee argues he has not received what he deserves).

Fraud can be classified into three types: "fraudulent reporting," "safeguarding of assets," and "corruption" [32]. "Fraudulent reporting" concerns deliberate misstatements or omissions of amounts or disclosures (e.g., adjustment of accounting records). "Safeguarding of assets" includes protecting entities' assets (e.g., property, cash) from theft. "Corruption" covers bribery and other illegal acts.

B. BUSINESS PROCESS MANAGEMENT

BPM is "a structured approach employing methods, policies, metrics, management practices, and software tools to coordinate and continuously optimize an organization's activities and processes" [33]. This approach consists of analyzing, designing, implementing, and continuously improving the business processes of organizations [34]. Business processes (BP) can be defined as an assembly of interrelated events, activities, and decision points that involve a number of actors (human actors such as suppliers, employees, and customers along with organizations and software systems) and objects (such as equipment, materials, products, paper documents, electronic documents, and electronic records) to achieve an outcome that is of value to at least one customer [15]. These form the ingredients of the business process, as shown in Fig. 1. Because each process ingredient can be exposed to fraud, PBF assessment should consider them all. Successful fraud detection efforts should consider the entire business process and identify where fraud might originate [35].

III. LITERATURE REVIEW

A. METHOD

A systematic literature review was conducted as follows:

1. ***First-round literature review:*** A preliminary manuscript search was conducted on Google Scholar, Science Direct, IEEE Xplore, Springer Link, Web of Science, and ProQuest Computing databases using initial keywords[3] to obtain an overview of the topic and check for duplicates.
2. ***Keyword refinement[4]:*** The initial keywords were refined by considering the keywords of the studies identified in step 1. Additionally, synonyms of the keywords were included to make the search more comprehensive.
3. ***Inclusion criteria:*** In this step, the inclusion criteria were defined for selecting relevant papers. The inclusion criteria stipulated the inclusion of any research article that explicitly dealt with fraud detection in business processes.
4. ***Second-round literature review:*** A new search was conducted on the target library databases (mentioned in step 1) using the refined list of keywords. All research results that met the inclusion criteria from step 3 were retained. The last search was conducted on February 13, 2019.
5. ***Backward and forward searches:*** A backward and forward search was conducted on the studies found in step 4, examining the references in both the selected studies (backward search) and the studies that cite them (forward search).
6. ***Result update:*** The alerts feature in Google Scholar was used to receive notifications about new studies that satisfied the inclusion criteria.

ATLAS.ti software[5] was used for analyzing the literature. The ATLAS.ti software is a qualitative data analysis software that supports literature analysis [36].

B. RESULTS

Table 1 summarizes the results of the literature search. Ultimately, 75 studies were selected and analyzed.

The first-round literature review yielded five results without duplicates. Three results were from Google Scholar and one result each from the IEEE Xplore and Web of Science databases.

The second-round literature review produced 54 results:

- Google Scholar produced 17,900 results. The first 400 results were checked. Most of the results after the first 100 were not relevant to the topic of PBF detection. After reviewing the results, 36 studies were selected.
- ScienceDirect produced 85 results. The advanced search feature was used to refine the results by searching for "fraud" in the "title, abstract or keywords" field. After reviewing the results, two studies were selected.

[3] The initial search keywords are: fraud AND (BPM OR "business process") AND (metrics OR indicators OR measures OR detection) AND ("literature review" OR review).

[4] The final search keywords are: fraud AND (BPM OR "business process") AND (assess OR metrics OR symptoms OR indicators OR patterns OR KPIs OR measures OR "red flags" OR detection).

[5] www.atlasti.com.

TABLE 1. Literature review search results.

Digital library	Number of results	Number of selected results from the first-round literature review	Number of selected results from the second-round literature review
Google Scholar	400	3	36
Science Direct	85	0	2
IEEE Xplore	19	1	5
Springer Link	27	0	2
Web of Science	26	1	4
ProQuest Computing	152	0	1
Number of selected results from backward and forward searches	21		
Total number of selected results	76		

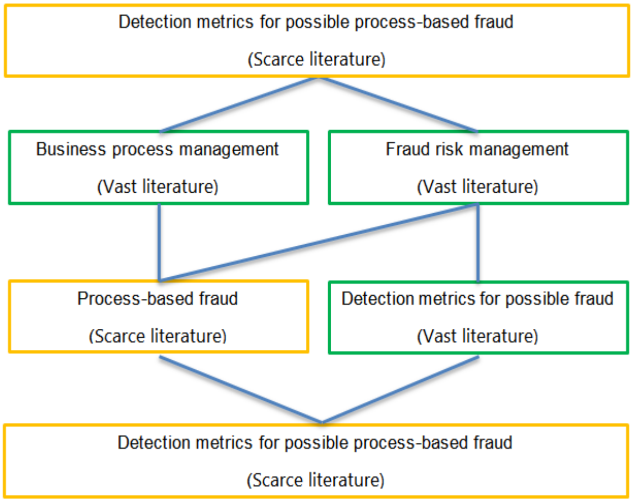
Detection metrics for possible process-based fraud
(Scarce literature)
Business process management
(Vast literature)
Fraud risk management
(Vast literature)
Process-based fraud
(Scarce literature)
Detection metrics for possible fraud
(Vast literature)
Detection metrics for possible process-based fraud
(Scarce literature)

FIGURE 2. Literature map.

- IEEE Xplore produced 19 results. After reviewing the results, five studies were selected.
- Springer Link produced 27 results. The advanced search feature was used to search for "fraud" in the "title" field. After reviewing, two studies were selected.
- Web of Science produced 26 results. Of these, four studies were selected.
- ProQuest Computing produced 152 results by using the "document title" field in the advanced search section. However, news as a source type was excluded. After reviewing the results and discarding duplicate results from other databases, one study was selected.
- Backward and forward searches performed on the selected results yielded an additional three references. Furthermore, 18 references about the general fraud detection technical techniques were added by using backward and forward searches. Although these references implicitly mentioned PBF detection, they are needed to cover the general technical methods of fraud detection in order to make this literature review comprehensive.

Fig. 2 summarizes the results of the content analysis by mapping the relevant topics and presenting their status in terms of their frequency in the literature. It indicates that the topics "detection metrics for possible fraud" and "detection metrics for possible process-based fraud" are closely related. Thus, the following subsections review these topics.

1) DETECTION METRICS FOR POSSIBLE FRAUD

The most successful and common metrics used for fraud detection are the "red flags" [8], [30]. Red flags are a collection of circumstances that are extraordinary or deviate from the usual state [30]. Red flags are signs of potentially fraudulent behavior because they indicate that something irregular may have occurred [37]. A red flag is only a pointer that an investigation is needed [30]; it cannot confirm the existence of fraudulent activity [38]. The Statement on Auditing Standards No. 99 (AICPA, 2012a) asks external auditors to utilize red flags to detect fraudulent financial reporting [39].

The red flags in SAS No. 99 are classified by the fraud triangle theory as follows [38]: (1) pressure red flags that measure deviance from certain specified goals; (2) opportunity red flags that measure how much responsibility or oversight is missing; and (3) rationalization red flags that measure a perpetrator's internal justification for committing fraud by incorrect reasoning [39].

To examine the effectiveness of red flags for detecting fraud in SAS No. 99, Moyes *et al.* [39] conducted a survey of 52 internal and 40 external auditors. They found that red flags vary in effectiveness; specifically, opportunity red flags were identified by the external auditors as most significant in detecting fraud. To explore behavioral red flags, Sandhu [40] interviewed 26 individuals who had been personally involved in either a fraud investigation or a fraud observation. Interviewees highlighted the following behavioral characteristics as red flags: strong ambition, social aloofness, extended working hours, dissatisfaction with the current job, justification of unethical behavior, personal problems, and living standards disproportionate to current means.

Information Technology (IT) can help detect red flags, for example, when they are encoded to reflect expert rules and incorporated into a rule engine [8]. Moreover, the following analysis techniques can generally be useful for fraud detection [41]:

- ***Filtering:*** this technique enables the user to select only the suspect data rather than the complete data, which may be challenging to examine. For example, applying a filter to focus attention on transactions outside the norm.
- ***Using equations for recalculation:*** equations can be used to check values or examine logical relationships for validating the organization's final calculations. For example, auditors can apply an equation for calculating

the total price by multiplying the quantity by the unit price and comparing the result with the amount charged on each invoice.

- ***Finding gaps:*** searching for missing items in a series or sequence can help detect fraud. For example, finding gaps in check or purchase order numbers.
- ***Utilizing summary statistics (such as sums, averages, deviations, min-max values, sorting, grouping, and aggregating):*** statistical analysis can provide a quick summary of the data that reveals irregularities in the numeric fields before a detailed analysis begins. For example, sorting helps to find data outliers for further investigation.
- ***Finding duplicates in the data (such as duplicate suppliers, contracts, or invoices):*** this technique entails looking for duplicate data in fields that should contain unique values and, therefore, may require a fraud investigation. For example, duplicate invoice numbers may indicate that an invoice has been paid twice.
- ***Using pivot tables:*** these tables are used to analyze the data from multiple dimensions to create a comprehensive view of the business. For example, creating a pivot table for employee payment transactions and combining it with the type of payments (salary, overtime, and shift premium) can reveal unusual combinations.
- ***Using trend analysis:*** this technique analyzes information from several years or locations to identify irregularities in the data. For example, the existence of many return transactions due to defects may indicate possible fraud in which someone is purchasing inferior goods and receiving a kickback from the vendor.
- ***Using regression analysis:*** regressions are used to predict values or to match actual values with predicted values to identify anomalies in the data. For example, a building manager receives cash for an apartment rental and fails to register the lease with the building owner. Regression analysis can be used to predict the number of apartments rented based on the usage of electricity or water.
- ***Using a simulation:*** this technique simulates a system's proper functioning for verification. For example, auditors can obtain the input data necessary for determining the correct employee benefit amounts and independently replicate the calculations done by the corresponding system to check if the benefit calculations have been altered to favor certain parties.

Furthermore, using IT through data mining-based methods is common for detecting fraud [12]. Data mining-based methods process large quantities of data to derive an underlying meaning [42]. These methods can be categorized into six main categories: classification, clustering, regression, outlier detection, visualization, and prediction [43], [44], as cited in [12]. In addition, data mining methods combine multiple techniques from other domains such as statistics, machine learning, high-performance computing, and many application domains [45]. Numerous data mining methods that have been commonly used for detecting fraud are described in Table 2. These methods can be used alone or combined with other techniques to build a robust detection system [12].

The best way to use data mining methods for fraud detection is by using them for classifying suspicious transactions for further consideration [42]. However, data mining methods face some challenges that may obstruct their performance such as concept drifting (i.e., changes that happen over time), supporting real-time detection, skewed distribution (i.e., where there are many fewer samples of fraudulent cases than standard cases), the handling of a large amount of data, typical classification problems like feature selection and parameter tuning, and disproportionate misclassification cost [12], [47]. A technical comparison between the common data mining methods for detecting financial fraud is shown in Table 3 [42].

2) DETECTION METRICS FOR POSSIBLE PROCESS-BASED FRAUD

PBF can be detected when business processes deviate from standard operating procedures [11]. Although a simple deviation from the business process is not necessarily fraud, the deviation signals the need for further investigation to prove or disprove the existence of fraud.

Mueller-Wickop [59] and Schultz [60] conducted semi-structured interviews to identify the key information for auditing business processes; this information is summarized in Table 4 [17].

Business processes involve multiple perspectives [62]. First, the control-flow perspective represents the ordering of activities in the business process. Second, the resource perspective deals with the process resource that is responsible for transforming the process work. It includes issues such as roles, organizational units, and authorizations. Third, the data perspective highlights data matters in the process, including decisions, data creation, and forms. Fourth, the time perspective involves time-related issues such as any applicable durations and deadlines [62]. Fifth, the function perspective describes process activities and related applications. Lastly, the context perspective is related to process context issues such as location and the social context [63].

Business processes can be displayed in several presentation layers that highlight different information for process auditing, as shown in Table 5 [17].

The first layer is the process map that provides the information required to plan and define the scope for the overall audit. The process map provides an essential overview of the relevant processes by presenting process information in an aggregated form. It can be used at the planning stages of a business process audit [17]. An example process map diagram is shown in Fig. 3. In this process map, every business process is depicted as a separate line. The length of each process line corresponds to the number of distinct activities in the process, and thus immediately reflects the complexity of the process. The number attached to each colored line shows

TABLE 2. Data mining methods commonly used for detecting fraud.

Method	Description
Artificial neural network	A technique that works the same as a human's brain, as it stores knowledge and uses information when need it [46]. The information is split into different layers (inputs, hidden, and outputs) [46]. Each layer has multiple neurons that are connected with weighted edges [47]. The weights are adjusted during the learning phase to guess the correct class labels [48]. It can be taught to implement machine learning algorithms and pattern recognition for classification and prediction [49].
Logistic model, logistic regression	A technique of classifying binary data by using a linear model, which is known as a logistic or logit model, to execute regression on a set of variables [10]. It is useful for predicting the presence or absence of a characteristic or outcome based on a set of predictor variables [47]. Moreover, it is suitable for classification problems like fraud detection [50].
Support vector machine	A classification technique that converts a linear problem into a higher dimensional feature space to decrease computational complexity [42]. It can solve non-linear optimization problems such as data structuring problems for fraud detection [48]. It is mainly used for classification and prediction [50].
Decision tree, forest, and CART	An inductive technique that recursively distributes a set of data through a tree representation [46]. It represents possible solutions to end up with a choice based on certain conditions [47]. It is used for prediction and classification [50].
Genetic algorithm/ programming	A predictive technique that uses a scoring process to obtain the optimal solution [46], [47]. It is usually used for classification [50].
Text mining	A data mining technique that is performed on plain text to transform the data into a quantitative form such as word frequency and word combinations [42]. After developing the quantitative form, the traditional data mining method is applied for classification [42]. It is commonly used for clustering and anomaly detection [50].
Group method of data handling	An induction data mining technique that finds the optimal solution through increasingly generated and validated models using a linear regression technique [42].
Response-surface methodology	A method for constructing global approximation to system behavior [51]. It is used for determining the best-applied method to the problem domain [50].
Self-organizing map	A form of artificial neural networks that has a single matrix of neurons [42].
Bayesian belief network	A statistical technique that makes use of the Bayes theorem that determines the probability that a given hypothesis is correct [42]. The technique is probabilistic and separates the joint probability distribution of a set of variables using local dependencies into factors [52]. It is commonly used for prediction and anomaly detection [50].
Process mining	A methodology that is used to discover, monitor, and improve real processes by analyzing their event logs [53]. It partially automates the process queries by linking the actual processes with their data and the process models [54].
Artificial immune system	A data mining technique that imitates the behavior of the biological immune system to detect antigens, for example, by creating detector cells to detect foreign bodies [42]. It is commonly used for anomaly detection [50].
Hybrid methods	A technique that uses a combination of multiple traditional techniques by selecting beneficial attributes of each to create a superior algorithm [42].
Deep learning	A machine learning technique that delivers excellent performance and flexibility by learning to represent data as a nested hierarchy of concepts within layers of the neural network [55]. It is similar to the neural network principle, with many hidden layers [47]. It exceeds traditional machine learning as the scale of data increases; however, it is still an active research technique that is currently getting considerable attention [55].
Graph embedding	A network representation learning (RL) technique that aims to convert the nodes in a network into low-dimensional vector spaces while maintaining the original properties of the network [56]. It can automatically extract useful information that will be used as generated features together with a baseline fraud detection model of a network into a vector space [57]. It is currently an active research topic that can be directed to exploring non-linear models, studying the evolution of networks, and generate artificial networks with real-world characteristics [58].

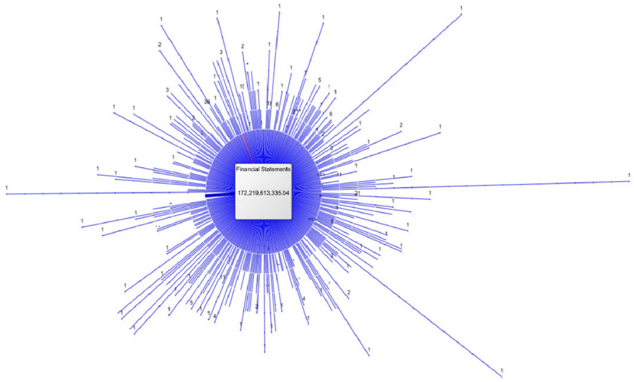

FIGURE 3. Example of a process map. Source: [17].

the frequency of each business process, where the color heat map ranging from low (blue) to high (red) depicts relative frequency. Line thickness shows the portion of the overall posting volume produced by a process. The figure shows that a total volume of 172,219,613,335.04 is posted in the financial accounts by 362 business processes.

The second layer is the stream layer; it can be used to zoom in from the overall process map to a more detailed level. It enables examination of a collection of business processes that affect specific financial accounts or sets of accounts (such as payable accounts). Organization auditors may give more attention to business processes with a high fraud risk such as the order-to-cash cycle, the procure-to-pay cycle, payroll, and inventory processes [64]. Focusing on high-risk financial accounts inside the business process could reveal suspicious account pairings, such as debt to depreciation [64]. An example of a process stream is shown in Fig. 4. It represents the set of business processes that generated journal entries on a particular account. The represented processes account for a total posting volume of 3,079,735.88.10 on the payables account 160000. Every business process instance is depicted as a separate line (similar to the process map) as follows: The length of the line shows the complexity of the process;

TABLE 3. Relevant properties of data mining methods for financial fraud. detection. Source: [42].

Method	Strengths	Limitations
Neural network	Well established history with fraud detection. Proven suitability with other non-algorithmic, binary classification problems.	Requires high computational power for training and operation, making it unsuitable for real-time function. Potential for overfitting if training set is not a good representation of the problem domain, so requires constant retraining to adapt to new methods of fraud.
Logistic model	Simple to implement. Well established history with fraud detection.	Lower classification performance than other data mining methods, difficulty with the complexity of fraud detection.
Support vector machine	Capable of solving non-linear classification problems like fraud detection. Training and operation requires low computational power, which gives potential for real-time operation.	Difficult for auditors to process results due to transformation of input set.
Decision trees, forests, and CART	Simple to implement and understand. Training and operation requires low computational power, which gives potential for real-time operation.	Potential for overfitting if training set is not a good representation of the problem domain, so requires constant retraining to adapt to new methods of fraud. Optimization during initial setup requires high computational power.
Genetic algorithm/ programming	Simple to implement using classification accuracy as the fitness solution. Proven suitability with other non-algorithmic, binary classification problems.	Requires high computational power for training and operation, making it unsuitable for real-time function. Difficulty adapting to new fraud methods due to local maxima/minima problem.
Text mining	Highly useful for fraud types with large amounts of textual data, such as financial statement fraud.	Requires another classification method to perform the actual fraud detection. Textual data are typically more subjective, and thus harder to process.
Group method of data handling	Simple to implement. Guaranteed to provide the best available solution.	Difficulty classifying noisy data, which many fraud types contain.
Response-surface methodology	Capable of solving non-linear classification problems like fraud detection.	Lower classification performance than other data mining methods, difficulty with complexity of fraud detection.
Self-organizing map	Simple to implement and very easy for auditors to understand given visual nature of results.	Visualization requires auditor observation, cannot be fully automated easily.
Bayesian belief network	Proven suitability with other non-algorithmic, binary classification problems. High computational efficiency gives potential for real- time operation.	Requires strong understanding of typical and abnormal behavior for the investigated fraud type.
Process mining	Useful for internal fraud investigations where information is available for every iterative step. Ability to focus on an entire process chain instead of individual attributes.	Requires strong understanding of typical and abnormal behavior for the investigated fraud type. Difficulty classifying noisy data, which many fraud types contain.
Artificial immune system	High suitability for classification problems with imbalanced data, such as fraud detection.	Requires high computational power for operation, making it unsuitable for real-time function.
Hybrid methods	Adaptive to new fraud techniques by combining the strengths of multiple traditional detection methods.	Fraud is a high-cost problem and therefore new, under-tested methods carry a large amount of risk.

TABLE 3. *(Continued)* Relevant properties of data mining methods for financial fraud. detection. Source: [42].

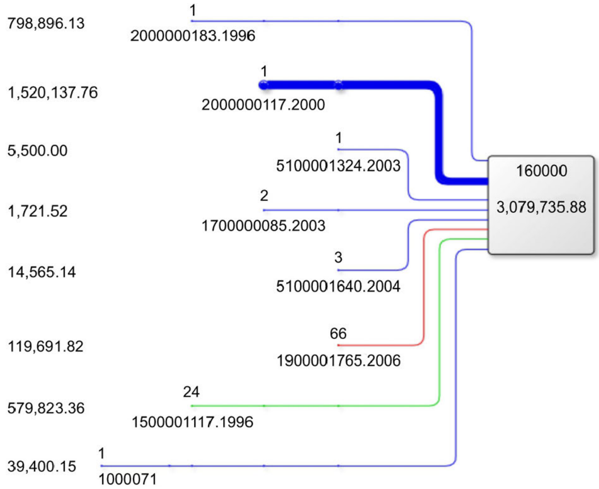

FIGURE 4. Example of a process stream. Source: [17].

the number attached to the upper end of each line and color shows the frequency of the business process, and the numbers at the lower end reflect the process IDs; the thickness of a line shows the total posting volume that was created by the process; and the numbers to the left of each process show the overall posting volume from each process.

The third layer is the process model that provides detailed information about the activities executed within the process model. This detailed information enables the process auditor to detect any invalid, inaccurate, incomplete, or unauthorized transactions [17]. Furthermore, it helps the auditor examine if a particular control works [17]. The fourth layer is the instance model that provides information about data entries produced by a particular execution of a business process. The instance layer can be used to understand the audit trail in an information system. Additionally, it can be used to examine the effectiveness of internal controls and to identify

TABLE 4. Key information concepts for auditing business processes. Adapted from [17].

Concept	Explanation
Process Flow	Information about the different activities in a process and how they are related.
Controls	Controls affect the operation of business processes and ensure activities are performed in accordance with management expectations. Controls can be classified as preventive, detective, and corrective. Controls can be implemented in information systems (application controls), performed as manual controls, or implemented via organizational structures.
Organizational aspects	This refers to organizational units, like departments, or resources. For example, an audit should identify individuals who interact in a business process.
Financial Statements	These represent information about the economic situation and performance of the reporting entity. They consist of the balance sheet (BS), profit and loss statement (P&L), cash flow statement, and additional appendices. Financial accounts record the results of business activities. The BS and P&L list the financial accounts and their adjusted balances at the end of a reporting period in a structured way.
Information Systems	These are the information and computer technologies used to operate business activities, and record and store the relevant accounting data.
Data	Includes any input or output information produced and stored in the source information systems during the operation of business processes, and which are relevant to financial accounting.
Materiality	Materiality is defined in ISA 320 as follows: “Misstatements, including omissions, are considered to be material if they, individually or in the aggregate, could reasonably be expected to influence the economic decisions of users taken by the financial statements.” [61] Auditors use the concept of materiality to assess which transactions or groups of transactions need auditing and evaluate their impact on the financial statements if compliance violations are detected.

TABLE 5. Representation layers of business processes. Adapted from [17].

Presentation layer	Representing	Information provided on	Related Information
Process Map	All processes All accounts	The general process structure The relationship between business processes and the BS and P&L The materiality of business processes The information systems supporting business processes The aggregate posting volumes created by different business processes	Process Flow Financial Statements Materiality & Information Systems Data
Process Stream	Many processes One account or group of accounts	The general process structure The relationship between business processes and a selected financial account or group of accounts The materiality of business processes The aggregate posting volumes created by the different business processes	Process Flow Financial Statements Materiality Data
Process Model	One process Many accounts	The detailed process structure The internal controls embedded in the process The relationship between the business process and financial accounts Users involved in the process The aggregate posting volumes created by the process	Process Flow Controls Financial Statements Organizational Aspects Data
Instance Model	One instance Many accounts	The detailed process structure The internal controls embedded in the process The relationship between the business process instance and financial accounts Users involved in the process The concrete journal entries and related data entries created by the process	Process Flow Controls Financial Statements Organizational Aspects Data

and evaluate the impact of process deviations or compliance violations [17].

In the literature, there are many implementation techniques for detecting fraud in business processes. Jans *et al.* [65] proposed a method for detecting possible PBF by using process mining techniques but omitted a technical implementation. The method uses some detection metrics for possible PBF by considering the use of control flow analysis, role analysis, and performance analysis to examine business process deviations. Stoop [66] proposed the $1 + 5 + 1$ concept, which consists of: (1) log preparation + (5) {a} log analysis, {b} performance analysis, {c} social analysis, {d} conformance analysis, and {e} process analysis using sorting, summarization, joining and aging, filters, summarization + (1) refocusing, and iteration. Even when the $1 + 5 + 1$ concept is used, process-based fraud cannot be detected automatically and human experts are needed. Samo *et al.* [67] used process mining algorithms and hybrid association rule learning (ARL) to implement some compliance checking rules with weights for detecting possible fraud. The process mining algorithms were used to detect deviations in the process model, and ARL algorithms were used to detect fraudulent behavior as an additional metric. However, this was done subjectively. Huda *et al.* [68] applied fuzzy logic to detect low deviations, where judgment on whether the deviation is fraudulent is based on a fraud rating. An improved study by Huda *et al.* [11] included the behavior of the event originator as a metric to increase precision and showed that the behavior of the originator metric could increase the accuracy level by 3%. However, all these techniques are still not sufficiently able to detect possible fraud [11].

The literature review reveals that fraud detection techniques are usually built based on the anomaly, misuse, or hybrid detecting approaches, as depicted in Fig. 5 [12].

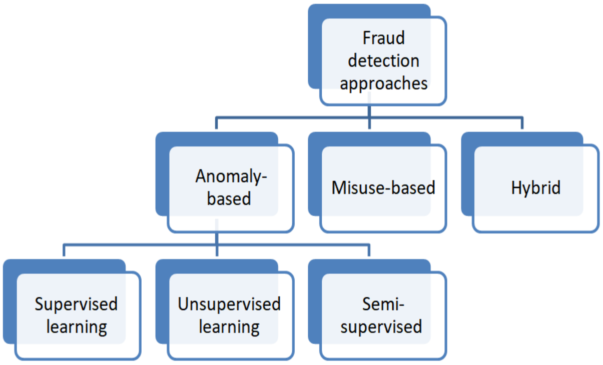

FIGURE 5. Fraud detection approaches.

Anomaly-based fraud detection is performed by capturing any deviation from normal or safe behavior [69]. This approach can help detect new fraud but suffers from a lack of generalization capability and the presence of high false alarm rates [70]. This approach is commonly implemented by three machine learning techniques: supervised, unsupervised, and semi-supervised [71]. First, the supervised learning technique requires data to be labeled as ''fraud'' and ''nonfraud'' and involves training a classifier. It is the most popular technique, and it has the advantages of being meaningful to humans and is easy to use regarding discriminative pattern classification and data regression. However, it has some limitations, such as the difficulty of collecting and finding distinctive labels. Second, the unsupervised learning technique does not require predefined labeled data, as there is no class label for model construction. It delivers a new explanation or representation of the observed data to improved future decisions [47]. The unsupervised learning technique detects fraud under the assumption that most of the cases in the dataset are nonfraud. However, the advantage of not relying on accurate identification for labeled data is limited by the problem of deception by camouflage techniques that seem to comply with normal behavior [8]. Third, the semi-supervised learning technique is situated between supervised and unsupervised learning. It delivers better performance compared to supervised learning, as it includes some labeled data and a large amount of unlabeled data. In addition, the misuse-based fraud detection approach is built by using known patterns of misuse to detect any suspicious transaction. It is an expert system that considers a fast and straightforward detection approach but is limited to the known patterns of misuse [12]. Lastly, the hybrid approach of misuse and anomaly detection combines anomaly-based and misuse-based fraud detection [12]. Selecting the best approach depends on the application domain and the case situation [72]. However, the anomaly-based approach is the most common [12].

Table 6 summarizes the literature on the detection metrics for possible fraud in business processes. Each metric is defined along with its respective reference studies. Most current PBF detection metrics mentioned in the literature have insufficient theoretical validation. Moreover, the current metrics do not fully address some essential conceptual business process perspectives, such as ingredients of a business process, business process perspectives, and business process presentation layers. However, all these conceptual perspectives should be used to develop metrics to ensure a complete and effective approach for detecting possible fraud in business processes. For example, by using the business process presentation layers, the current metric, the ''skipped activity,'' can be extended to cover skipped instances, skipped processes, and skipped streams. These extensive metrics can be used by the fraud examiners to enhance the review of possible PBF in organizations. Additionally, the tightening of the conceptual business process perspectives will enable the developers of the PBF detection techniques to have a holistic view of PBF detection that enables them to develop improved techniques for detecting PBF.

TABLE 6. Fraud detection metrics in business processes.

ID	Metric name	Explanation	Reference
1	Skipped Activity	Not performing an activity that should be executed as stated in the standard operating procedure (SOP). The skipped activity is either routine or a decision activity [73].	[6], [11], [13], [67], [68], [73], [74]
2	Wrong Resources	The activity is performed by an actor that is not defined in the SOP.	[6], [11], [13], [67], [68], [73]–[75]
3	Wrong Duty	The same actor executes different activities, which should require different privileges. This includes “wrong duty sequence” in the sequence activity, “wrong duty decision” in the decision activity and “combined wrong duty” in the sequence and decision activities [73].	[6], [11], [13], [67], [68], [73], [74]
4	Wrong Pattern	Deviation from the standard sequence as stated in the SOP.	[6], [11], [13], [67], [68], [73]–[75]
5	Wrong Decision	The decision activity execution is a deviation from standard decision execution as stated in the SOP.	[6], [11], [13], [67], [68], [73], [74]
6	Wrong Throughput Time	The activity execution time deviates from the standard time as stated in the SOP. It includes “wrong throughput time min” and “wrong throughput time max” [73].	[6], [11], [13], [67], [68], [73], [74]
7	Parallel event	Nonparallel events are performed at the same time.	[11], [68]
8	Originator behavior	The behavior of the actor while executing the activity is anomalous.	[11], [67], [68]

IV. CONCLUSION

This study offers a better understanding of the current state of fraud detection by concentrating on fraud in business processes that operationalize organizational strategies to promote future efforts of researchers and practitioners in this critical research field. It identifies the most relevant topics and examines the existing metrics by conducting a systematic literature review. The literature review yielded 76 studies that were selected and analyzed by using content analysis to provide a firm theoretical foundation for adequate fraud detection in business processes. This includes specifying the most critical conceptual perspectives to be considered in detecting PBF that are components of a business process, business process perspectives, critical information for auditing the business process, and business process presentation layers.

The proposed literature map reveals that both BPM and fraud risk management are the primary domains of this study, and they have received considerable attention in the literature. Although a large body of research has examined detection metrics for possible fraud (e.g., ''red flags''), less attention has been paid to PBF, which found that fraud can be detected when business processes deviate from standard operating procedures. The detection metrics for possible PBF, which are commonly implemented by using process and data mining methods, have also received little attention in the literature. Only eight detection metrics for possible fraud in business processes (skipped activity, wrong resources, wrong duty, wrong pattern, wrong decision, wrong throughput time, parallel event, and originator behavior) are found in the literature review. These metrics do not address the needs of the different conceptual perspectives on business processes and have insufficient theoretical validation. A successful fraud detection approach should tightly integrate the conceptual perspectives of business processes. This substantiates the need for future research to extend the current detection metrics of PBF.

In future research, extending fraud detection metrics in business processes with an evaluation of their effectiveness of exposing common fraud risks will be proposed. Furthermore, a case study of specific business contexts will be conducted where organizations apply and validate certain metrics as a supplement to PBF detection models.

REFERENCES

[1] M. Werner, N. Gehrke, and M. Nuttgens, ''Business process mining and reconstruction for financial audits,'' in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Hamburg, Germany, Jan. 2012, pp. 5350–5359.

[2] D. S. Kerr and U. S. Murthy, ''The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey,'' *Inf. Manage.*, vol. 50, no. 7, pp. 590–597, Nov. 2013.

[3] S. Y. Huang, C.-C. Lin, A.-A. Chiu, and D. C. Yen, ''Fraud detection using fraud triangle risk factors,'' *Inf. Syst. Frontiers*, vol. 19, no. 6, pp. 1343–1356, Dec. 2017.

[4] *Annual Fraud Indicator 2017*, Crowe UK, London, U.K., 2017.

[5] D. Al-Jumeily, A. Hussain, A. Macdermott, G. Seeckts, and J. Lunn, ''Methods and techniques to support the development of fraud detection system,'' in *Proc. Int. Conf. Syst., Signals Image Process. (IWSSIP)*, Sep. 2015, pp. 224–227.

[6] E. S. Pane, A. D. Wibawa, and M. H. Purnomo, ''Event log-based fraud rating using interval type-2 fuzzy sets in fuzzy AHP,'' in *Proc. IEEE Region Conf. (TENCON)*, Nov. 2016, pp. 1965–1968.

[7] F. Sinaga and R. Sarno, ''Business process Anomali detection using multi-level class association rule learning,'' *IPTEK J. Proc. Ser.*, vol. 2, no. 1, pp. 1–2, Jan. 2016.

[8] B. Baesens, V. Van Vlasselaer, and W. Verbeke, *Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques: A Guide to Data Science for Fraud Detection*. Hoboken, NJ, USA: Wiley, 2015.

[9] V. Van Vlasselaer, T. Eliassi-Rad, L. Akoglu, M. Snoeck, and B. Baesens, ''GOTCHA! Network-based fraud detection for social security fraud,'' *Manage. Sci.*, vol. 63, no. 9, pp. 3090–3110, Sep. 2017.

[10] E. Ngai, Y. Hu, Y. Wong, Y. Chen, and X. Sun, ''The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature,'' *Decis. Support Syst.*, vol. 50, no. 3, pp. 559–569, Feb. 2011.

[11] S. Huda, R. Sarno, and T. Ahmad, ''Increasing accuracy of process-based fraud detection using a behavior model,'' *Int. J. Softw. Eng. Appl.*, vol. 10, no. 5, pp. 175–188, May 2016.

[12] A. Abdallah, M. A. Maarof, and A. Zainal, ''Fraud detection system: A survey,'' *J. Netw. Comput. Appl.*, vol. 68, pp. 90–113, Jun. 2016.

[13] S. Huda, T. Ahmad, R. Sarno, and H. A. Santoso, ''Identification of process-based fraud patterns in credit application,'' in *Proc. 2nd Int. Conf. Inf. Commun. Technol. (ICoICT)*, May 2014, pp. 84–89.

[14] B. Wetzstein, ''KPI-related monitoring, analysis, and adaptation of business processes,'' Univ. Stuttgart, Stuttgart, Germany, Tech. Rep., 2016, doi: 10.18419/opus-8956.

[15] M. Dumas, M. La Rosa, J. Mendling, and H. A. Reijers, *Fundamentals of Business Process Management*. New York, NY, USA: Springer, 2013.

[16] R. Davis and E. Brabander, *ARIS Design Platform: Getting Started With BPM*. London, U.K.: Springer, 2007.

[17] M. Werner, ''Process model representation layers for financial audits,'' in *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, Mar. 2016, pp. 5338–5347.

[18] D. Cotton, S. Johnigan, and L. Givarz, *Fraud Risk Management Guide*. New York, NY, USA: COSO, 2016.

[19] M. J. Nigrini, *Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations*. Hoboken, NJ, USA: Wiley, 2011.

[20] L. Finkelstein and M. Leaning, ''A review of the fundamental concepts of measurement,'' *Measurement*, vol. 2, no. 1, pp. 25–34, Jan. 1984.

[21] J. Cardoso, ''Business process control-flow complexity: Metric, evaluation, and validation,'' *Int. J. Web Services Res.*, vol. 5, no. 2, pp. 49–76, Apr. 2008.

[22] A. Ljungberg, ''Process measurement,'' *Int. J. Phys. Distrib. Logistic Manag.*, vol. 32, no. 4, pp. 254–287, 2002.

[23] A. Neely, M. Gregory, and K. Platts, ''Performance measurement system design: A literature review and research agenda,'' *Int. J. Oper. Prod. Manag.*, vol. 15, no. 4, pp. 80–116, Apr. 1995.

[24] V. C. Yen, ''An integrated model for business process measurement,'' *Bus. Process Manage. J.*, vol. 15, no. 6, pp. 865–875, Nov. 2009.

[25] M. Leyer, D. Heckl, and J. Moormann, ''Process performance measurement,'' in *Handbook on Business Process Management*, vol. 2. Berlin, Germany: Springer, 2015, pp. 227–241.

[26] N. E. Fenton and S. L. Pfleeger, *Software Metrics: A Rigorous and Practical Approach*, vol. 2. Boston, MA, USA: PWS Publishing, 1997.

[27] M. Z. Muehlen and R. Shapiro, ''Business process analytics,'' in *Handbook on Business Process Management*, vol. 2. Berlin, Germany: Springer, 2015, pp. 243–263.

[28] G. Polancic and B. Cegnar, ''Complexity metrics for process models—A systematic literature review,'' *Comput. Standards Inter.*, vol. 51, pp. 104–117, Mar. 2017.

[29] G. Muketha, A. Ghani, M. Selamat, and R. Atan, ''A survey of business process complexity metrics,'' *Inf. Technol. J.*, vol. 9, no. 7, pp. 1336–1344, Jul. 2010.

[30] T. P. DiNapoli, ''Red Flags for Fraud,'' State New York Office State Comptroller, New York, NY, USA, Tech. Rep., 2008. [Online]. Available: https://www2.osc.state.ny.us/localgov/pubs/red_flags_fraud.pdf

[31] M. B. Clinard and D. R. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement*, vol. 19, no. 3. Montclair, NJ, USA: Patterson Smith, 1954.

[32] *Committee of Sponsoring Organizations of the Treadway Commission, Internal Control-Integrated Framework: Internal Control Over External Financial Reporting: A Compendium of Approaches and Examples*, Committee of Sponsoring Organizations of the Treadway Commission, Durham, NC, USA, 2013.

[33] A.-W. Scheer and E. Brabänder, ''The process of business process management,'' in *Handbook on Business Process Management*, vol. 2. Berlin, Germany: Springer, 2010, pp. 239–265.

[34] J. vom Brocke and M. Rosemann, *Business Process Management* (Wiley Encyclopedia of Management). Hoboken, NJ, USA: Wiley, 2015.

[35] R. Nisbet, G. Miner, and K. Yale, ''Fraud detection,'' in *Handbook of Statistical Analysis and Data Mining Applications*. Amsterdam, The Netherlands: Elsevier, 2018, pp. 289–302.

[36] J. vom Brocke, P. Fettke, M. Gau, C. Houy, and S. Morana, ''Tool-support for design science research: Design principles and instantiation,'' *SSRN Electron. J.*, vol. 2015, pp. 1–13, May 2017.

[37] G. Baader and H. Krcmar, "Reducing false positives in fraud detection: Combining the red flag approach with process mining," *Int. J. Accounting Inf. Syst.*, vol. 31, pp. 1–16, Dec. 2018.

[38] E. Yucel, "Effectiveness of red flags in detecting fraudulent financial reporting: An application in Turkey," *J. Account. Finance*, no. 60, pp. 139–158, 2013. [Online]. Available: http://www.journal.mufad.org/ and http://www.journal.mufad.org.tr/attachments/article/716/9.pdf

[39] G. D. Moyes, R. Young, and H. F. M. Din, "Malaysian internal and external auditor perceptions of the effectiveness of red flags for detecting fraud," *Int. J. Audit. Technol.*, vol. 1, no. 1, p. 91, 2013.

[40] N. Sandhu, "Behavioural red flags of fraud—A qualitative assessment," *J. Hum. Values*, vol. 22, no. 3, pp. 221–237, Sep. 2016.

[41] D. Coderre, *Computer Aided Fraud Prevention and Detection: A Step by Step Guide*. Hoboken, NJ, USA: Wiley, 2009.

[42] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Comput. Secur.*, vol. 57, pp. 47–66, Mar. 2016.

[43] H. Edelstein. *Data Mining: Exploiting the Hidden Trends in Your Data*. Accessed: 1997. [Online]. Available: http//wwww.db2mag.com/db_area/archives

[44] N. M. Mohamad, S. H. Ab Hamid, R. Mohemad, M. M. A. Jali, and M. S. Hitam, "A review on a classification framework for supporting decision making in crime prevention," *J. Artif. Intell.*, vol. 8, no. 1, pp. 17–34, Jan. 2015.

[45] J. Han, J. Pei, and M. Kamber, *Data Mining: Concepts and Techniques*. Waltham, MA, USA: Elsevier, 2011.

[46] G. Suresh and R. J. Raj, "A study on credit card fraud detection using data mining techniques," *Int. J. Data Min. Tech. Appl.*, vol. 7, no. 1, pp. 21–24, 2018.

[47] V. Patil and U. K. Lilhore, "A survey on different data mining & machine learning methods for credit card fraud detection," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3, no. 5, pp. 320–325, 2018.

[48] X. Zhou, S. Cheng, M. Zhu, C. Guo, S. Zhou, P. Xu, Z. Xue, and W. Zhang, "A state of the art survey of data mining-based fraud detection and credit scoring," *MATEC Web Conf.*, vol. 189, Aug. 2018, Art. no. 03002.

[49] K. Kamusweke, M. Nyirenda, and M. Kabemba, "Data mining for fraud detection in large scale financial transactions," *EasyChair*, no. 1729, Oct. 2019. [Online]. Available: https://mail.easychair.org/publications/preprint_download/G5sK

[50] J. West, M. Bhattacharya, and R. Islam, "Intelligent financial fraud detection practices: An investigation," in *Proc. Int. Conf. Secur. Privacy Commun. Netw.* Cham, Switzerland: Springer, 2015, pp. 186–203.

[51] W. Zhou and G. Kapoor, "Detecting evolutionary financial statement fraud," *Decis. Support Syst.*, vol. 50, no. 3, pp. 570–575, Feb. 2011.

[52] N. Khakzad, F. Khan, and P. Amyotte, "Risk-based design of process systems using discrete-time Bayesian networks," *Rel. Eng. Syst. Saf.*, vol. 109, pp. 5–17, Jan. 2013.

[53] G. Vossen, "The process mining manifesto—An interview with Wil van der Aalst," *Inf. Syst.*, vol. 37, no. 3, pp. 288–290 May 2012.

[54] S.-M.-R. Beheshti, *Process Analytics*. Cham, Switzerland: Springer, 2016.

[55] R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," Jan. 2019, *arXiv:1901.03407*. [Online]. Available: https://arxiv.org/abs/1901.03407

[56] Z. Zhang, "ANRL: Attributed network representation learning via deep neural networks," in *Proc. 27th Int. Joint Conf. Artif. Intell.*, vol. 1, Jul. 2018, pp. 3155–3161.

[57] S. Zhou, "Empirical effect of graph embeddings on fraud detection/risk mitigation," Mar. 2019, *arXiv:1903.05976*. [Online]. Available: https://arxiv.org/abs/1903.05976

[58] P. Goyal and E. Ferrara, "Graph embedding techniques, applications, and performance: A survey," *Knowl.-Based Syst.*, vol. 151, pp. 78–94, Jul. 2018.

[59] N. Mueller-Wickop and M. Schultz, "Towards key concepts for process audits—A multi-method research approach," in *Proc. 10th ICESAL*, Jun. 2013, pp. 70–92.

[60] M. Schultz, N. Müller-Wickop, and M. Nüttgens, "Key information requirements for process audits—An expert perspective," in *Emisa*, 2012, pp. 137–150.

[61] IAASB, "ISA 320 materiality in planning and performing an audit," *Int. Stand. Audit.*, vol. 1, pp. 313–321, May 2009.

[62] W. M. P. van der Aalst, "Business process management?: A comprehensive survey," *ISRN Softw. Eng.*, vol. 2013, pp. 1–37, 2013.

[63] J. Recker and J. Mendling, "The state of the art of business process management research as published in the BPM conference," *Bus. Inf. Syst. Eng.*, vol. 58, no. 1, pp. 55–72, Feb. 2016.

[64] A. Misra and V. Walden, "Proactive fraud analysis," *Intern. Audit.*, vol. 73, no. 2, pp. 33–37, 2016.

[65] M. Jans, J. M. Van Der Werf, N. Lybaert, and K. Vanhoof, "A business process mining application for internal transaction fraud mitigation," *Expert Syst. Appl.*, vol. 38, no. 10, pp. 13351–13359, Sep. 2011.

[66] J. J. Stoop, "Process mining and fraud detection—A case study on the theoretical and practical value of using process mining for the detection of fraudulent behavior in the procurement process," M.S. thesis, Twente Univ., Enschede, The Netherlands, 2012.

[67] R. Sarno, R. D. Dewandono, T. Ahmad, M. F. Naufal, and F. Sinaga, "Hybrid association rule learning and process mining for fraud detection," *IAENG Int. J. Comput. Sci.*, vol. 42, no. 2, pp. 59–72, Apr. 2015.

[68] S. Huda, R. Sarno, and T. Ahmad, "Fuzzy MADM approach for rating of process-based fraud," *J. ICT Res. Appl.*, vol. 9, no. 2, pp. 111–128, Nov. 2015.

[69] V. Jyothsna, "A review of anomaly based intrusion detection systems," *Int. J. Comput. Appl.*, vol. 28, no. 7, pp. 975–8887, 2011.

[70] K. Mule and M. Kulkarni, "Credit card fraud detection using Hidden Markov Model (HMM)," *Int. J. Innov. Technol. Adapt. Manag.*, vol. 1, no. 6, pp. 37–48, 2014.

[71] J. Akhilomen, "Data mining application for cyber credit-card fraud detection system," in *Proc. Ind. Conf. Data Mining*, 2013, pp. 218–228.

[72] S. Mardani and H. Shahriari, "Fraud detection in process-aware information systems using process mining," in *Proc. E-Syst. 21st Century*. New York, NY, USA: Academic, 2016, pp. 307–344.

[73] R. Sarno and F. P. Sinaga, "Business process anomaly detection using ontology-based process modelling and multi-level class association rule learning," in *Proc. Int. Conf. Comput., Control, Informat. Appl. (IC3INA)*, Oct. 2015, pp. 12–17.

[74] D. Rahmawati, R. Sarno, C. Fatichah, and D. Sunaryono, "Fraud detection on event log of bank financial credit business process using hidden Markov model algorithm," in *Proc. 3rd Int. Conf. Sci. Inf. Technol. (ICSITech)*, Oct. 2017, pp. 35–40.

[75] H. A. Hartanto, R. Sarno, and N. F. Ariyani, "Linked warning criterion on ontology-based key performance indicators," in *Proc. Int. Seminar Appl. Technol. Inf. Commun. (ISemantic)*, Aug. 2016, pp. 211–216.

[76] A. Van Looy and A. Shafagatova, "Business process performance measurement: A structured literature review of indicators, measures and metrics," *Springerplus*, vol. 5, no. 1, p. 1797, Dec. 2016.

BADR OMAIR was born in Riyadh, Saudi Arabia, in 1982. He received the B.S. and M.S. degrees in information systems from King Saud University, in 2004 and 2008, respectively, where he is currently pursuing the Ph.D. degree in information systems with a focus on fraud in business processes. His research interests include business process management, fraud detection, process mining, and design science research methodology in information systems.

AHMAD ALTURKI was born in Riyadh, Saudi Arabia, in 1978. He received the B.S. degree in information systems from King Saud University, Saudi Arabia, in 2000, and the M.S. and Ph.D. degrees in information systems from the Queensland University of Technology, in 2009 and 2014, respectively.

He is currently an Assistant Professor with the Department of Information Systems, King Saud University, where he has been, since 2014. He is the author of more than ten published articles. He is also a scientific reviewer of two journals and two conferences. His research interests include business process management, entrepreneurship, design research in information systems, enterprise resource planning systems, and design science research methodology in information systems.

Dr. Alturki was a recipient of the Best Dissertation Award from the Australian Council of Professors and Heads of Information Systems (ACPHIS), in 2014.

• • •